SK:AFM
F.#2016R02228

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH 12 EMAIL ACCOUNTS AND SIX OTHER ELECTRONIC ACCOUNTS THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, DROPBOX, LINKEDIN, AND ATLASSIAN	**TO BE FILED UNDER SEAL** **APPLICATION FOR SEARCH WARRANTS FOR INFORMATION IN POSSESSION OF PROVIDERS** Case No. 17-M-561

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANTS

I, EVELINA ASLANYAN, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for search warrants for information associated with certain accounts that is stored at premises controlled by Google, LinkedIn, Atlassian, and Dropbox (the "Providers"), electronic providers headquartered in the United States. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Providers to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since March 2012. I am responsible for conducting and assisting in investigations involving cybercrime. I have investigated and otherwise participated in numerous matters during the course of which I have conducted physical surveillance, interviewed witnesses, executed court-authorized search warrants and used other investigative techniques to secure relevant information. I am familiar with the facts and circumstances set forth below from my participation in the investigation, my review of the investigative file, and from reports of witnesses and other law enforcement officers involved in the investigation.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to search the information associated with certain electronic accounts and servers further described in Attachment A for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1030(a)-(b) (computer fraud and conspiracy and attempt to commit the same), 1343 and 1349 (wire fraud and wire fraud conspiracy), further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The FBI is investigating a massive and continuing fraud scheme known as "Metan," through which cybercriminals have siphoned away millions of dollars from U.S. companies.

7. The investigation so far has revealed that the scheme has been carried out in three stages, each of which has involved defrauding advertisers by creating the false impression that their online advertisements are being viewed or clicked on by human Internet users.

8. In the first stage, from approximately July 2014 to approximately September 2015, the conspirators used computers that they controlled to fraudulently click on advertisements and then took a share of the resulting revenue.

9. In the second stage, from approximately September 2015 to December 2016. the conspirators again defrauded advertisers. This time, the conspirators employed forged registration data to disguise their machines as the computers of real individuals browsing the Internet. They used these camouflaged machines, not to click on links, but to fabricate impressions of display ads[1] and video ads. They accomplished this by loading the advertisements on their own computers while sending falsified data up the commercial chain toward the advertisers, conveying the false impression that these non-existent Internet users were viewing the ads on premium websites. The conspirators pocketed the resulting

[1] "Display" advertisements, also known as banner advertisements, are online advertisements that typically consist of an image and associated text.

revenue. The second stage of the scheme ended when a cybersecurity firm publicly revealed the IP addresses of the computers that the conspirators were using to carry out the fraud, leading to those addresses' being blacklisted within the online advertising industry.

10. In the third stage, which began in or around November 2016 and is still being carried out, the conspirators are still committing display and video advertising fraud, but are doing so using third-party computers that are infected with malware.

11. The operators of the Metan system are mostly in Russia and the former Soviet Union, or are Russian expatriates living elsewhere. Where necessary, emails in Russian have been translated into English for purposes of this affidavit. These are draft translations.

a. Prior Search Warrant

12. On or about March 10, 2017, the Honorable Ramon E. Reyes, United States Magistrate Judge for the Eastern District of New York, signed search warrants authorizing the search of the following email accounts: adw0rds.yandex.ru@gmail.com, inno_rr@yahoo.com, ibetters@me.com, and mathete.com@gmail.com.

b. Background

(i) The Digital Advertising Market

13. Online services and websites are typically supported by advertisements. For example, while users of Google's search engine pay no fee to carry out web searches, Google charges advertisers to place advertisements among its search results. Similarly, users can browse many news and entertainment websites such as CNN.com for free because these sites charge advertisers to place advertisements on the sites. Within the online advertising industry, the term "publishers" is used to describe providers of content like Google or CNN. Broadly speaking, advertisers seek to place advertisements with publishers so that the ads can be seen and/or clicked on by human viewers who are drawn to the publishers' content.

14. Online advertisements can be divided into two categories. First, some advertisers rely on clickable links which, when clicked, bring the user to the advertiser's site. Advertisers typically pay each time such an ad is clicked on, a pricing model known as "cost per click" or "CPC." By contrast, other advertisers rely on content (such as images or videos) which appears in an allocated space within a webpage so that users encounter it in the midst of browsing. Because such content does not need to be clicked on to make an impact on viewers, the advertiser does not pay only for clicks, but instead pays every time a user loads a page on which the ad has been placed—a pricing model known as "cost per thousand impressions" or "CPM."

15. Publishers obtain ads from advertisers (via a long chain of intermediaries) using a short string of computer code called an "ad tag" that is embedded in the code making

up the publisher's web page.[2] The ad tag does not itself contain an ad; rather, it triggers the process that determines what advertisement will be shown in a designated spot on the page. The ad tag is furnished by an entity called an ad network that serves as an intermediary between the publisher and the pool of potential advertisers.

16. When a user loads a webpage, and the user's web browser encounters an ad tag, there ensues a split-second auction in which multiple advertisers bid for the opportunity to show an ad to that particular user on that particular web page. Agents for potential advertisers receive information that includes the user's internet service provider; his or her IP address; and the website that he or she was visiting when he or she clicked the link that led to the request to load the ad. This last piece of information, known as the "referer," is crucial because the identity of the website last visited by the user sends a signal about the user's value and also may correlate with the user's destination, where the ad will ultimately be shown.[3] The referer's identity is conveyed by the user's computer in a short message known as a "referer header."

17. When an advertiser "wins" this auction, its ad is uploaded from a separate computer (known as an "ad server") into the spot on the web page indicated by the ad tag. All of this takes place in microseconds, without the awareness of the user who is loading the

---

[2] In practice, the publisher may instead incorporate a "frame" into which a shifting series of ad tag code may be uploaded without the publisher's intervention.

[3] For instance, a user whose referer-header indicates that he has just visited CNN.com may well be headed toward a sub-page of CNN, such as CNN.com/domestic.

web page. The advertiser then pays the various intermediaries involved, as well as the publisher.

18. On any given web page, there may be multiple pieces of advertising "real estate" to be filled in this way. A website whose advertising real estate is highly desirable may be able to fill all of its ad slots in these split-second auctions (known as a "100% fill"). A website whose real estate is less desirable may achieve a lower rate of "fill."

19. An ad network has an incentive to place its ad tag on as many websites as possible to maximize revenues. In order to achieve this, the ad network may contract with another ad network (known as an "extended ad network") that has its own relationships with publishers. The extended ad network agrees to place the primary network's ad tag on the websites of the extended network's affiliated publishers, in return for a share of the resultant revenue.

(ii) The Fraudulent Schemes

20. Based on my review of the evidence in the investigation so far, including email records, network traffic information, subscriber information from online services, and information from cybersecurity researchers, the Metan conspirators have perpetrated an advertising fraud scheme that has taken several different forms over the past few years.

21. As set forth below, the instant scheme began as click fraud (the "Click Fraud Scheme"). In click fraud, malicious actors make money by directing computers they control to click on advertisements that have been placed on a cost-per-click basis. The advertisers then receive all or a share of the payments for these clicks.

22. With time, though, the scheme evolved to a new effort to defraud advertisers through fraudulent impressions of display and video advertisements (the "Display/Video Ad Fraud Scheme"). In this second scheme, rather than clicking on CPC ads, the fraudulent traffic directed by the conspirators would load, and purport to view or play, CPM ads. The conspirators referred to these schemes (both the Click Fraud Scheme and the Display/Video Ad Fraud Scheme) as "*Metan*," the Russian word for "Methane," As a front for their activities, the conspirators used Mediamethane, an ad network owned by Alexander Zhukov.

23. In preparation for the Display/Video Ad Fraud Scheme, the Metan conspirators acquired approximately 500,000 IP addresses, for which they created false registration information so that the addresses appeared to belong to real Internet users. A cybersecurity firm gathered the information documenting these false registrations, and I have reviewed a sample of that documentation.

24. The conspirators posed as an extended ad network to gather ad tags belonging to both complicit and unsuspecting ad networks. The conspirators then used the IP addresses they controlled to load these ad tags in such a way as to make it falsely appear to advertisers that the ad tags were being launched under circumstances justifying a high bid on the ads, when in fact the ads were not being seen by anyone. They did so, first, by sending false referer headers indicating that these hundreds of thousands of simulated Internet users were requesting the advertisers' ads after having visited websites such as nfl.com and oprah.com.[4]

---

[4] As noted above, a user who has just visited a high-value website is of value both because he is likely to visit other such websites and because, in practice, most online clicks that are placed on a high-value website only serve to move the user deeper into that same website, as

Having won the auctions, the conspirators then sent fraudulent requests to relevant ad servers that reinforced the appearance the ads were being served to these high-value websites.

25. The Display/Video Ad Fraud Scheme ended in December 2016, when the cybersecurity firm White Ops published a list of the IP addresses involved.

26. In or around November 2016, however, the Metan conspirators appear to have begun a new scheme—the "Hybrid Scheme"—that engaged in display and video ad fraud using a refinement of the conspirators' earlier technology.

27. The Hybrid Scheme resembles the previous schemes in that video and display ads are again being accessed by bots. However, the Hybrid Scheme employs victim computers that have been infected with malware, allowing the conspirators to funnel fraudulent traffic through them.

28. With regard to all of their schemes, the conspirators took measures to circumvent the third-party fraud detection services that many advertisers use to verify that they are not paying for fraudulent traffic. When a video ad is played on the computer of a putative Internet user, sophisticated verification software often scrutinizes the computer viewing the ad to ensure that it bears some indicia of human use. For example, based on statistical patterns of Internet usage, vendors of verification software expect to see that a certain percentage of viewers of an advertisement are also using Facebook at the same time. The conspirators took steps to ensure that the requisite percentage of the phantom "users"

---

when a browser on nytimes.com moves from one article to another. Thus, the referer-header, while it nominally conveys information only about the origins of an Internet user, also tells a story about the user's likely destination.

viewing the ads would show signs of Facebook use. Similarly, because traffic that originates only in the United States is a red flag that the traffic is of fraudulent origin, the conspirators sought to ensure that the supposed Internet users visiting the advertisements appeared to come from a number of countries. The conspirators also worked with co-conspirators at complicit ad networks to selectively block the anti-fraud code from loading in such a way that the verification companies would not be aware that their detection software had been evaded.

29. The investigation so far has revealed the following central players in the Click Fraud, Display/Video Ad Fraud, and Hybrid Schemes:

- **Alexander Zhukov** directed the Click Fraud and Display/Video Ad Fraud schemes and served as the CEO of Mediamethane, an associated company that posed as an extended ad network. Zhukov was in charge of the Metan team's relationships and communications with third parties, including co-conspirators.
- **Boris Timokhin** served as the chief programmer for the scheme.
- **Mikhail Andreev** provided early programming assistance in developing the Click Fraud Scheme.
- **Dmtri Novikov** provided early programming assistance in developing the Click Fraud Scheme.
- **Denis Avdeev** participated in the Click Fraud and Display/Video Ad Fraud Schemes and appears to have served as a technical liaison to network administrators at other companies.
- **Sergey Ovsyannikov** operated AdZos and Clickandia, entities that engaged in the Click Fraud, Display/Video Ad Fraud, and Hybrid Schemes.

c. The Click Fraud Scheme

30. Evidence indicates that the development of the Click Fraud Scheme began during the summer of 2014.

31. On or about July 17, 2014, Boris Timokhin ("Timokhin")[5] sent emails to Mikhail Andreev (using the email account x11org@gmail.com), Dmitry Novikov (using the email account whitelotusoflove@yandex.ru), and an unknown individual identified only as "Alexey." The emails contained a formal document outlining the ground rules for a "partnership" whose purpose was not described, but which would include conversion of funds into cryptocurrencies as necessary. The venture described in the document was to use a company called VBBB, which is known through open sources to be associated with Alexander Zhukov ("Zhukov").

32. Thereafter, as set forth below, numerous emails regarding click fraud were exchanged between Timokhin, Andreev, Novikov, and Zhukov.

33. The conspirators were assisted by two outside [redacted]. Both entities appear to have coached the conspirators in how to make the Metan botnet's fraudulent clicks appear to be human-generated.

---

[5] Unless otherwise specified, for all emails discussed in this affidavit, Timokhin used the email address mathete.com@gmail.com.

(i) Contribution of Clickandia to the Click Fraud Scheme

34. For example, on or about October 22, 2014, Dmitri Novikov wrote a posting in an internal communications group used by the conspirators to track progress on the click fraud project, within a project-tracking tool called Jira.

35. Jira is a product of the Atlassian Corporation. Users of Jira, and of a related Atlassian product called Confluence, are assigned usernames which may be used to store some of their message content in servers maintained by Atlassian. Messages created using these tools and found in the conspirators' email accounts, indicate that Andreev's Atlassian username was "Adw0rd"; Zhukov's username was "Nastra"; Novikov's usernames were "Listentome" and "Legefix"; and Timokhn's username was "Mathete." Messages sent through Jira and Confluence among the conspirators generally originated in a single email address (that appears to have been shared among the conspirators): assembla@betaggregator.com. From there, the messages were emailed out to the other conspirators.

36. Novikov's posting quoted a message he had apparently received from an email address called "tech@clickandia.net." As quoted in Novikov's posting, the Clickandia contact had stated: "you don't have 'accept' language in your headers while clicking. We don't have this kind of verification anymore, but a lot of providers have it. Hence accept-language for a search and a click must be identical." Novikov annotated this feedback as follows: "you need to add accept-language to a header while clicking."

37. Based on my training and experience, in these exchanges, Clickandia was giving the Metan conspirators advice on how to make the botnet's clicks look more like

human clicks. Specifically, the message from Clickandia indicated that many ad networks would only accept a click as valid if the browser that was carrying out the click emitted a short string of text (known as the "accept-language header") indicating the putative user's preferred language. If the Internet users simulated by Metan did not provide this information, their clicks would not register as real.

38. Another relevant exchange occurred on or about November 13, 2014, when Novikov updated a Confluence status tracker that was laid out in the form of a grid. In the row marked "Clickandia," in a column marked "Current issues," Novikov inserted the comment "Discussing mouse move." In a column marked "Click status," Novikov deleted the words "Not Clicking" and added "working."

39. Based on my training and experience, both of these comments relate to further refinements that the Metan team was making so that the clicks emanating from their botnet would appear to be coming from human Internet users. The note about "mouse move" related to an effort to remotely induce mouse movements in the computers that were clicking on Clickandia's links, so as to deceive advertisers' fraud-detection software by creating the illusion that there were humans at the controls of these computers. The change to "click status" meant that the bots' clicks on Clickandia's links were now being registered, as required to generate revenue.

40. Clickandia also appears to have been involved in video ad fraud. On or about October 28, 2014, Novikov wrote a message to Timokhin using Jira with the subject line "Emulating 'the viewing of a video.'" Novikov provided the URL "mycoolwebsite.net" and wrote, "Boris: Here [is where] Clickanda measures video."

41. Mikhail Andreev (who was one of the recipients of Timokhin's July 17, 2014 contract) appears to have provided technical assistance to the Metan team in bypassing the third-party verification vendors who were vetting Clickandia's traffic. On or about November 27, 2014, Andreev wrote a note in Confluence, providing computer code "to bypass their filter."

42. On or about May 8, 2015, Andreev used the email address x11org@gmail.com to send Timokhin an email entitled "USD account." The email contained United States correspondent banking account information for an account in Andreev's name at the Russian bank Alfabank.

(ii) Contribution of Affiliate Harbour to the Click Fraud Scheme

43. Crucial assistance in the development of the Click Fraud Scheme was also provided by [redacted], which appears to have commissioned the Metan botnet to click on ads belonging to [redacted], and also to have provided extensive technical support toward that goal.

44. For example, in a to-do list that Zhukov (using his ibetters2@gmail.com email account) sent to Timokhin on or about June 25, 2015, Zhukov made frequent reference to the complaints and demands of [redacted] and other partners.

45. In one item, Zhukov directed Timokhin "to find [the] [redacted] checker and see why they are complaining." Zhukov said that [redacted] had complained about a lack of "mouse move," and passed on some computer code that he said [redacted] had "given for friendship's sake."

46. Zhukov also noted that another entity had complained about "fake Chrome and mouse move."

47. Based on my training and experience, Zhukov was passing on a request from [redacted] that Timokhin locate and neutralize a piece of third-party software intended to identify fraudulent web traffic (known as a "checker" or "pixel"), because the software was leading to the denial of payment for the botnet's clicks on advertisements placed by [redacted], thus depriving both [redacted] and Metan of revenue. [redacted] had advised Zhukov that the software was detecting a lack of "mouse move," i.e. human-seeming mouse movements, and Zhukov noted that another partner had complained about detecting "fake Chrome," meaning that the clicks did not come from full-fledged Chrome web browsers such as a human browsing the Internet would use, but rather from simulated browser software operating on bots which were not truly viewing the ads in question. Zhukov indicated that "for friendship's sake," [redacted] had passed along tips for drafting computer code to resolve some of these problems.

48. Finally, in another item in the same list, Zhukov asked Timokhin "to add authorization for Facebook [] users. There is Google, twitter too; [but] no FB (There should be approximately 40% of them.)" Based on my training and experience, Zhukov was telling Timokhin that in order for the bots' clicks to appear real to fraud detection firms, at least 40% of the computers in the network had to appear to be signed into Facebook. Zhukov also indicated that this effort had already been undertaken with respect to Twitter and Google.

49. Numerous other emails reflect the efforts of [redacted] to assist the Metan conspirators with the click fraud scheme. For example, on or about June 29, 2015,

Zhukov (using his ibetters2@gmail.com account) emailed Timokhin an exchange that Zhukov had had with [redacted], in which [redacted] wrote: "Let's try to understand why the bot flies by the detection URLs… you need to understand that you cannot bypass the most simple of filters when the URL that you switch to changes." Based on my training and experience, in this exchange [redacted] was helping Zhukov to redesign Metan so that it could "bypass," or evade, the various third-party programs or "filters" designed to detect nonhuman traffic.

d. Zhukov Forges Internet Pedigrees for Metan's Simulated Internet Users

50. As discussed above, a key element of both the Click Fraud and Display/Video Ad Fraud Schemes was that real Internet users had to appear to be clicking on or viewing the ads, when in fact the ads were being clicked on by Metan's bots (in the case of the Click Fraud Scheme) or viewed and played by the bots (in the case of the Display/Video Ad Fraud Scheme). Moreover, high-value characteristics were chosen for these non-existent users so that they would command a high price from ad networks. To accomplish this, the conspirators disguised the internet service providers to which their supposed Internet users subscribed.

51. The conspirators accomplished this with the aid of IP address leasing companies which had the ability to modify entries in a worldwide directory attributing IP addresses to companies.

52. For example, on or about April 24, 2016, Zhukov (using the email address alex@tipsters.com) forwarded Timokhin an email exchange that Zhukov had engaged in with a representative of an IP address leasing company.

53. In that exchange, the leasing company confirmed false directory information provided by Zhukov that incorrectly listed [redacted] as the controller of an IP address when, in fact, it was Zhukov who controlled the IP address.

54. Based on my training and experience, the effect of this false directory entry, in combination with the many other false entries that the conspirators created, was to create the impression that the simulated Internet users clicking on links or viewing display and video ads were a disparate group of real individuals, many connecting to the Internet as customers of Internet service providers that showed them to be high-value viewers. If the advertisers had been aware of the reality that the machines "watching" the ads were accessing the Internet from a block of IP addresses that was under common control, this would have served as a clear tipoff that the clicks and ad impressions were fraudulent and therefore worthless.

e. The Display/Video Ad Fraud Scheme

55. Approximately during the summer of 2015, the Metan conspirators began to develop the Display/Video Ad Fraud Scheme. Rather than profit from fraudulent clicks, the Metan conspirators would heretofore seek to generate fraudulent views, meaning that they would deceive advertisers into thinking that their ads had been viewed by humans, when in fact they had not. Individual instances in which an ad is viewed by an Internet user are known in the industry as "impressions."

56. In order to "view" display ads and "play" video advertisements, the conspirators made use of the disguised IP addresses they controlled.

57. However, in a departure from the click fraud scheme, Metan's phantom Internet users did not actually travel around the web to commit display and video ad fraud.

Rather, each of the Metan bots simply transmitted a referer header that (falsely) indicated that it had just visited a high-value website, touching off the split-second auction discussed above. The Metan system then transmitted a message to the appropriate ad server that purported to download the ad to a page on that high-value website, cementing the false impression that a user was browsing the site. In fact, the page to which the ad server transmitted the ad was a forgery that resided on Metan's servers, and not on the high-value website.

58. An email from Zhukov (using ibetters2@gmail.com) to Timokhin, dated October 17, 2016, displays the Metan team's attempts to refine both elements of this scheme—the non-existent high-value users and the forged high-value websites—using feedback from [redacted], a co-conspirator [redacted] further discussed below whose name the conspirators sometimes abbreviated as [redacted]

59. Zhukov commented to Timokhin that "We agreed with [redacted] – 75%. Additionally, they are helping." He added: "They made a note that the traffic is 100% US. This immediately strikes the Buyer as a sign that it's a bot. The second sign: Equal domain distribution 5% 5% 5%. It needs to be totally random."

60. Based on my training and experience, this email lays out the rough financial terms of Metan's relationship with [redacted] and also passes on [redacted]'s suggested refinements to the scheme. First, Zhukov commented that [redacted] would be giving Metan its ad tags so that Metan could create fraudulent ad impressions against ads provided by [redacted] clients. In return, [redacted] would give the Metan team 25% of the resultant revenue while keeping 75% for itself.

61. Second, Zhukov related two areas in which the Display/Video Ad Fraud Scheme must improve. First, the phantom Internet users simulated by Metan must appear to hail from a range of countries, rather than being "100% US." Second, the browsing habits of these nonexistent Internet users should be realistically "random," rather than segmented among websites in rigidly fixed percentages ("5% 5% 5%").

(i) The Metan Team Accepts Orders for Referers

62. As discussed, the conspirators were deceiving advertisers (and other players in the Internet advertising ecosystem) into believing that ads were being viewed on real websites. Websites that are both highly trafficked and high "fill" generate more advertising revenue than poorly trafficked, low-fill sites, since the advertising real estate on such websites is both expensive and densely occupied.

63. The Metan conspirators sought to fabricate high-value referers for their non-existent Internet users. Moreover, they customized these fraudulent website lists at the request of the different ad networks they conspired with, in an effort to simulate, for each ad network, the websites which would give that network the highest "fill."

64. Many of the telltale communications underlying this scheme involve an ad network providing the Metan conspirators with (1) an ad tag (to permit the uploading of ad content) and (2) a long list of high-fill websites.

65. Based on my knowledge, training, and experience, and consultation with individuals in the advertising industry, in legitimate commerce, an extended ad network can only place ads with publishers with whom it has a relationship. Thus, before requesting placement from an extended ad network, the requesting network would have to first inquire

about the extended network's portfolio of relationships, and tailor its request accordingly. But the Metan team's communications with ad networks did not fit this model. Rather, and tellingly, the Metan team appeared able to accept unrestricted requests from Mediamethane's partners for ad placement, without limitations as to publisher.

66. For example, on or about October 18, 2016, Zhukov (using his a@mediamethane.com email account) exchanged emails with an individual named [redacted] who used the email address [redacted].

67. In an email with the subject line "Business Partnership," [redacted] introduced himself and then sent Zhukov an ad tag, along with a lengthy list of high-traffic websites (such as [redacted].com, [redacted].com, [redacted].com, and [redacted].com). [redacted] wrote to Zhukov: "Please find the high filling domains across the different platforms we use. See if you have access to these domains and drive more traffic."

68. Based on my training and experience, this instruction would not be given in a legitimate business context because an extended ad network that lacked Metan's ability to forge ad placement would not simply "have access" to the domains on an extensive list of high-traffic websites.

69. Other communications with external partners similarly indicate that the Metan team was unconstrained by normal technical and business limitations. For example, on or about June 23, 2015, Zhukov (using his ibetters2@gmail.com email account) received an email from an individual named [redacted], who used the email address [redacted]. [redacted]f provided an ad tag and cautioned Zhukov as follows:

"Here is the new feed as I promised. Please limit it to around 3mil searches per day for now."

70. Based on my training and experience, in this communication, [redacted] was reversing the normal business logic of the advertising industry. Rather than asking Zhukov to *maximize* traffic, [redacted] was asking Zhukov to *limit* the traffic on [redacted]'s ad tag—an instruction that would only make commercial sense in an environment where Zhukov was able to direct unlimited amounts of Internet traffic to websites of his choosing, to an extent that might have caused technical difficulties or raised the concern of traffic verification companies.

71. Evidence from the execution of prior search warrants indicates that the Metan conspirators corresponded with [redacted] employees from June 23, 2015 to November 24, 2015.

(ii) Zhukov Accepts Orders From [redacted] For Websites to Run Ads On

72. In addition to taking orders from companies like [redacted] and [redacted], the Metan conspirators also worked on a partnership basis with some ad networks that not only solicited fraudulent Internet traffic, but also provided crucial assistance in refining Metan's fraud technology. Among these was a company called [redacted].

73. For example, on or about October 13, 2016, Zhukov (using the email address a@mediamethane.com) emailed [redacted], a [redacted] employee whose email address is [redacted]. Zhukov wrote, "Send me please fresh top 20 refers domain for USA prerolls."

74. [redacted] responded, "Here [are] the top USA desktop domains nowadays," along with a list of major websites, such as [redacted], and others.

75. Zhukov, again using his Mediamethane email account, then forwarded [redacted]'s email to Timokhin, commenting, "Add please fresh refers in place of the old ones for [redacted] Timokhin responded: "DONE."

76. Based on my training and experience, in this exchange Zhukov solicited from [redacted] a newly updated (or "fresh") list of the websites (or "refers") with the highest fill and/or traffic at that moment. [redacted] then sent the requested list to Zhukov, and Zhukov in turn asked Timokhin to fraudulently create the appearance that users were visiting these websites and watching ads on them, in place of a prior list of websites ("the old ones").

77. A similar exchange occurred on October 14, 2016, when Zhukov (using his ibetters2@gmail.com email account) forwarded Timokhin a similar list of prominent websites with the subject line "Top 30 from [redacted] and the note "Can be replaced." When Zhukov thanked Timokhin for adding these sites, Timokhin wrote, "We are doing it for the money." In apparent agreement, Zhukov responded: "Glory to having balls… In the end, cash conquered evil."

78. Based on my training and experience, in this exchange Zhukov was replacing the prior list of high-fill websites with a newly updated list provided by [redacted] ([redacted]). When Zhukov thanked Timokhin for implementing the change, Timokhin pointed out that these thanks were unnecessary, since they were both out to make money.

79. Similarly, on October 27, 2016, Zhukov (using his a@mediamethane email address) forwarded to Timokhin an email that he had received from an individual using the

name [redacted] and the email address [redacted]. [redacted] sent Zhukov a list of web domains with the preface: "Bro… Any way you can change to run these sites please," which Zhukov passed on to Timokhin, noting, "Add new referres to the [redacted] please."

80. Based on my training and experience, "[redacted] is an abbreviation for "[redacted]," indicating that [redacted] worked at [redacted].

81. On or about October 16, 2016, Zhukov used his ibetters2@gmail.com account to forward Timokhin another communication that demonstrated the degree of assistance [redacted] was supplying to the Metan conspirators.

82. In the forwarded communication, which was a log of an online chat, Zhukov was conversing with an individual identifying himself as "[redacted]."

83. In the exchange, "[redacted]" and Zhukov (identified as "Aleksandr Zh") discussed "checks" using "Fraudlogix" and "MOAT" and "IAS," and Zhukov queried whether he needed to "get [a] report… to see where we have to make fixes." [redacted] responded: "I checked today and nothing… shows no alerts."

84. Zhukov transmitted this exchange to Timokhin with the subject "a moment of vanity." Zhukov then added the prefatory comment, "Metan is magnificent" and the following postscript: "Made friends with the [redacted].. he understands what kind of solution we have and he wants to work, and he is ready to cooperate[.]"

85. Based on my training and experience, in this exchange [redacted] (using the nickname "[redacted]") was helping Zhukov to evade various fraud detection services to which [redacted] had access, including those provided by Fraudlogix, Moat, and Integral

Ad Science ("IAS"). [redacted]t was reassuring Zhukov that the simulated traffic created by Metan was not running afoul of any of these services' fraud detection filters ("no alerts"). Zhukov, in turn, was excitedly relaying this result to Timokhin ("Metan is magnificent") and was also pointing out to Timokhin that [redacted] was fully colluding with Metan ("he is ready to cooperate").

86. The Metan co-conspirators appear to have advertised for partners and/or co-conspirators on LinkedIn, based on an email that Zhukov received on October 26, 2016 from a potential partner that began as follows: "We saw your posting on Linkedin." Zhukov received the email at his a@mediamethane.com email address, indicating that Zhukov used this address as the registration email for his LinkedIn account. Zhukov subsequently appears to have generated fraudulent ad traffic on behalf of the individual who contacted him via LinkedIn.

(iii) The Metan Conspirators Create Fraudulent Traffic for [redacted]

87. In addition to [redacted], the conspirators received orders for fraudulent Internet traffic from an advertising network they referred to as "[redacted]

88. [redacted] had apparently struck a deal whereby ads would be placed only on webpages that also bore certain keywords. Thus, in order to assist [redacted] in defrauding [redacted]'s advertiser clients, the Metan conspirators had to create specialized fraudulent pages with the necessary keywords for the bots to "visit."

89. On or about October 13, 2016, in an email with the subject line "new domains for feeds with filled in titles and keywords," Timokhin emailed Zhukov at his ibetters2@gmail.com account as follows: "It is my understanding that new domains were

sent for [redacted] But his feed has keywords. I.e., if there are no pages for the domain here - https://centbycent.com/meth/prerolls/prerollvideopage/, then we don't fill the feed at all and most likely, we get zero fill for this domain. In such cases, I send the domains to [redacted] and he puts the pages together and then I add them."

90. Based on my training and experience, Timokhin was outlining his plan for dealing with [redacted] need for keywords: Timokhin would have "[redacted] create false pages ("put[] the pages together") with the requisite keywords.

91. Later that same day, Zhukov (using his ibetters2@gmail.com address) emailed Timokhin a link to an image file that was stored on the Dropbox file storage service, at a URL that (based on information reported by Dropbox) is associated with Dropbox User ID [redacted]

92. Timokhin responded, "Everything got kinda worse in the past hours[.] Maybe we should go back to the… old domains with the keywords? Meanwhile, [redacted] will collect [keywords] today-tomorrow for the new pages?"

93. Zhukov wrote, "Let's cut them off completely for now… let them freak out a bit… and tomorrow, we will start with a clean slate." Timokhin responded: "I am cutting [redacted] off completely, and giving [redacted] the domains to get the keywords in there."

94. Based on my training and experience, in this exchange, Zhukov was conveying to Timokhin that their attempt to craft keyword-laden pages to help [redacted] had been unsuccessful. The image file that Zhukov sent Timokhin was most likely a screen capture showing a control panel with performance statistics for the Metan fraud. The solution that the Metan conspirators arrived at was to temporarily cease providing fraudulent

traffic for [redacted] and to use the interval to have Avdeev create fresh domains with new keywords.

95. Information obtained from Dropbox indicates that Zhukov controls the Dropbox account with User ID [redacted] The registered user of the account has email account i-betters@ya.ru, and goes by the name Alexander Zhuk.

f. **The Metan Conspirators Develop the Hybrid Scheme**

96. In December 2016, the cybersecurity firm [redacted] published a white paper revealing the Metan scheme (which [redacted] termed "Methbot") and disclosing the IP addresses that the Metan conspirators were using. In response, those IP addresses were blacklisted by cybersecurity firms, effectively ending the Display/Video Ad Fraud Scheme.

97. At the same time, however, the conspirators, or individuals who were associated with or learned from the conspirators, appear to have been developing a new scheme (the "Hybrid Scheme") that made use of victim's computers that had been infected with malware to load display and video ads for fraudulent purposes.

(i) The Hybrid Scheme is Linked to Adzos.com and Clickandia.com

98. The Hybrid Scheme was observed in or around April 2017 by the advertising infrastructure provider [redacted] discovered that when certain video ads were loaded, attempts were apparently being made to block fraud detection software. Upon further investigation, [redacted] determined that the affected advertisements had one thing in common: connections to an extended ad network called AdZos.

99. [redacted] gives its customers the ability to log in to a proprietary portal where they can monitor ad performance. [redacted]s customers use their email addresses as login

usernames. The [redacted] clients affiliated with AdZos were found to have supplied the email addresses support@adzos.com and sergey@adzos.com as usernames.

100. Information reported pursuant to a subpoena by the internet service provider Digital Ocean indicates that a user with the email address sergey@adzos.com has repeatedly signed into Digital Ocean from an IP address associated with AdZos and has, in the course of paying Digital Ocean's invoices, identified himself as Sergey Ovsyannikov.

101. AdZos appears to be under common control with Clickandia, the ad network whose operators assisted the Metan team in setting up their click fraud operation. According to Digital Ocean, Ovsyannikov also pays the bills for Clickandia.com. Moreover, the AdZos and Clickandia websites are identically designed in terms of graphics, formatting, and images, albeit with different text.

102. Logs of data traffic associated with the Hybrid Scheme contain identifiers that have also led investigators back to AdZos. These logs, assembled by the cybersecurity firm [redacted], show that the malicious actors appear to have been tracking their performance using Google Analytics, a website traffic analysis tool operated by Google.

103. Google Analytics users are assigned a "Tracking ID" for use in tracking the performance of online elements. A Tracking ID consists of the letters "UA," followed by a hyphen, followed by the user's Google Analytics account number, followed by a hyphen and a "property number" denoting the particular element being tracked.

104. The string UA-12145724-11 appears in the logs of malicious traffic.

105. Information provided by Google indicates that among the registered users of that Tracking ID are individuals with email addresses sergey@adzos.com and alex@adzos.com.

(ii) The Hybrid Scheme is Linked to Loscritino@gmail.com

106. In addition to the Adzos.com email accounts described above, Google has reported that Tracking ID UA-12145724-11 is associated with another relevant email account, loscritino@gmail.com, as well as a relevant web domain, mycoolwebsite.net. Each of these identifiers is associated with other elements of the fraud under investigation. Mycoolwebsite.net was identified by Dmitri Novikov in October 2014 as a site connected to Clickandia's efforts "to emulate 'the viewing of a video.'" See supra ¶ 40. A user with the username "loscritino" registered the domain names for both Mycoolwebsite.net and Clickandia.com, according to the domain name registrar Namecheap.

(iii) The Fraud Scheme is Linked to Qoqenator@gmail.com

107. According to information provided by Google, the email account qoqenator@gmail.com belongs to Timokhin. On or about October 2, 2014, Zhukov (using his a@vbbb.com email account) forwarded to qoqenator@gmail.com an email that Zhukov had received the previous day from Mikhail Andreev's email account, x11org@gmail.com. The email bore the subject "Fwd: urls" and included various website addresses, including mycoolwebsite.net, the website address linked to Google Analytics Tracking ID UA-12145724-11. Qoqenator@gmail.com is also the "recovery account" for Timokhin's email account mathete.com@gmail.com (used throughout the fraudulent schemes), meaning that

Timokhin registered qoqenator@gmail.com as the email address at which he wished to receive emails if the "mathete" account became inaccessible.

THE TARGET ACCOUNTS

108. This search warrant seeks authorization to search the following premises for the period July 1, 2014 to June 23, 2017.

a. Email Accounts:

i. **a@mediamethane.com**, hosted by Google, was the Mediamethane email address used by Alexander Zhukov, who appears to have directed the Click Fraud and Display/Video Ad Fraud Schemes. Zhukov often used this email address to communicate about the Metan schemes with co-conspirators at other businesses, including [redacted] Zhukov also received a message at this email address responding to a LinkedIn posting he had created seeking potential business partners.

ii. **alex@adzos.com,** hosted by Google, is one of the registered email accounts for Google Analytics Tracking ID UA-12145724-11, which appears in data traffic related to the Hybrid Scheme. Based on my knowledge, training, and experience, and my review of the workings of Google Analytics, individuals using Google Analytics receive real-time emails at their registered email accounts regarding performance of the website being tracked, revenue flow, traffic characteristics, other email addresses associated with the website, and changes in service to the account.

iii. **alex@tipsters.com**, hosted by Google, was used by Alexander Zhukov. Zhukov used this email address on or about April 24, 2016 to communicate about leasing an IP address with false registration information.

iv. **assembla@betaggregator.com**, hosted by Google, appears to have been a central "hub" email address that was used to centrally receive, and then retransmit to all the conspirators, updates made by the conspirators to their Jira or Confluence workflows

v. [redacted] hosted by Google, was used by [redacted] at [redacted] to communicate with the Metan conspirators about domain names to be used in the Display/Video Ad Fraud Scheme. In a non-email chat, [redacted] also

gave the Metan conspirators technical advice about defeating fraud detection systems.

vi. **ibetters2@gmail.com**, hosted by Google, was frequently used by Alexander Zhukov through the course of the fraudulent schemes for communications with his co-conspirators regarding the scheme.

vii. **loscritino@gmail.com**, hosted by Google, is one of the registered email accounts for Google Analytics Tracking ID UA-12145724-11, which appears in logs of recent malicious traffic associated with the Hybrid Scheme. In addition, the username "loscritino" was used to log in to the domain registrar Namecheap in order to register the websites Clickandia.com and mycoolwebsite.net As described above, the registered email account for a Google Analytics account typically receives real-time emails at their registered email accounts regarding performance of the website being tracked, revenue flow, traffic characteristics, other email addresses associated with the website, and changes in service to the account.

viii. **qoqenator@gmail.com**, hosted by Google, was used by Boris Timokhin and received an email regarding the fraudulent scheme from Zhukov. This email account is the "recovery account" for Timokhin's email account mathete.com@gmail.com (used throughout the fraudulent schemes), meaning that Timokhin registered qoqenator@gmail.com as the email address at which he wished to receive emails if the "mathete" account became inaccessible.

ix. **sergey@adzos.com**, hosted by Google, is the email of record for the website of the ad network AdZos, associated with video streams recently observed to have blocked antifraud software. This email account is one of the registered email accounts for Google Analytics Tracking ID UA-12145724-11, which appears in data traffic related to the Hybrid Scheme.

x. **support@adzos.com,** hosted by Google, is one of the email addresses used by AdZos employees to log into LKQD's online portal.

xi. **tech@clickandia.com** is an email address that corresponded frequently with the Metan conspirators regarding the Click Fraud scheme.

xii. **x11org@gmail.com** was used by Mikhail Andreev to communicate with the other Metan conspirators regarding the fraudulent schemes under investigation.

b. Other Premises:

i. **Atlassian username "Adw0rd**," a username in Confluence and Jira project-tracking software hosted by the Atlassian Corporation, was

used by Mikhail Andreev to communicate with the other Metan conspirators regarding the fraudulent schemes under investigation.

ii. **Atlassian username "Mathete,"** a username in Confluence and Jira project-tracking software hosted by the Atlassian Corporation, was used by Boris Timokhin to communicate with the other Metan conspirators regarding the fraudulent schemes under investigation.

iii. **Atlassian username "Nastra,"** a username in Confluence and Jira project-tracking software hosted by the Atlassian Corporation, was used by Alexander Zhukov to communicate with the other Metan conspirators regarding the fraudulent schemes under investigation.

iv. **Dropbox account with User ID 94568916** was used to host an image containing performance metrics for the Metan botnet and is registered to Alexander Zhukov.

v. **Google Analytics Account 12145724** was used to track the performance of the Hybrid Scheme. An associated Tracking ID, 12145724-11, is specifically associated with mycoolwebsite.net. a site that appears to have been used by Clickandia in connection with video ad fraud.

vi. **LinkedIn account registered to a@mediamethane.com**: Alexander Zhukov appears to have advertised for partners and/or co-conspirators using this LinkedIn account. The Metan botnet generated apparently fraudulent display/video ad traffic on behalf of a contact who first reached out to Zhukov via this LinkedIn account.

Therefore, based on my knowledge, training, and experience, and the facts set forth in this affidavit, there is probable cause to believe that each of the aforementioned premises contains evidence of the crimes under investigation.

BACKGROUND CONCERNING EMAIL

109. In my training and experience, I have learned that each of the Providers provides a variety of on-line services, including electronic mail ("email") access, to the public. Each of the Providers allows subscribers to obtain email accounts at certain domain names, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with the Providers. During the registration process, each of the Providers asks

subscribers to provide basic personal information. Therefore, the computers of the Providers are likely to contain stored electronic communications (including retrieved and unretrieved email for the Providers' subscribers) and information concerning subscribers and their use of the Providers' services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

110. A subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by the Providers. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

111. In addition, I am aware that providers offer services through which a computer user can search webpages for text that the user types in, and that under some circumstances the provider saves the user's text searches for later retrieval. I am also aware that providers may also keep records of the webpages or IP addresses that a user clicks on or types directly into his web browser's address bar (as opposed to the provider's search bar), if the user is using the provider's web browser (e.g., Google Chrome) and has logged into the web browser with his email account's username and password.

112. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account.

Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

113. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

114. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email

providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

115. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling investigators to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the

geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

BACKGROUND CONCERNING SERVERS

116. Server providers like Digital Ocean maintain server computers connected to the Internet. Their customers use those computers for a wide range of different purposes, including operating websites and providing cloud-based data storage. In general, providers like Linode ask each of their customers to provide certain identifying information when registering for services, including name, contact information, email address and business information. Providers like Linode also may retain records of the length of service (including start date) and types of services utilized. In addition, for paying customers, such companies typically retain information about the customers' means and source of payment for services (including any credit card or bank account information).

117. Server providers' customers typically place files, software code, databases and other data on the servers. To do this, customers connect from their own computers to the server computers across the Internet. This connection can occur in several ways. In some situations, it is possible for a customer to upload files using a special web site interface offered by the server provider. It is frequently also possible for the customer to directly

access the server computer through the Secure Shell ("SSH") or Telnet protocols. These protocols allow remote users to type commands to the web server. The SSH protocol can also be used to copy files to the server. Customers can also upload files through a different protocol, known as File Transfer Protocol ("FTP"). Servers often maintain logs of SSH, Telnet and FTP connections, showing the dates and times of the connections, the method of connecting, and the IP addresses of the remote users' computers (IP addresses are used to identify computers connected to the Internet). Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports.

118. The servers use those files, software code, databases and other data to respond to requests from Internet users for pages or other resources from the website. Commonly used terms to describe types of files sent by a server include HyperText Markup Language ("HTML") (a markup language for web content), Cascading Style Sheets ("CSS") (a language for styling web content), JavaScript (a programming language for code run on the client's browser), and image files. Server providers frequently allow their customers to store collections of data in databases. Software running on the server maintains those databases; two common such programs are named MySQL and PostgreSQL, although those are not the only ones.

119. Server providers sometimes provide their customers with email accounts; contents of those accounts are also stored on the company's servers.

120. Web sites deliver their content to users through the Hypertext Transfer Protocol ("HTTP").6 Every request for a page, image file, or other resource is made through an HTTP request between the client and the server. The server sometimes keeps a log of all of these HTTP requests that shows the client's IP address, the file or resource requested, the date and time of the request, and other related information, such as the type of Web browser the client uses.

121. Websites are often known to the outside world by a domain name, such as www.uscourts.gov or www.amazon.com. Domain names must be registered to particular individuals or entities. Sometimes, server providers offer customers the separate service of registering domain names. When that occurs, server providers typically retain information related to the domain name, including the date on which the domain was registered, the domain name itself, contact and billing information for the person or entity who registered the domain, administrative and technical contacts for the domain, and the method of payment tendered to secure and register the domain name.

122. In some cases, a subscriber or user will communicate directly with a server provider about issues relating to a website or account, such as technical problems, billing inquiries or complaints from other users. Server providers typically retain records about such communications, including records of contacts between the user and the company's support services, as well as records of any actions taken by the company or user as a result of the communications.

---

[6] This includes secure forms of HTTP, such as HTTPS.

BACKGROUND CONCERNING DROPBOX

123. Dropbox is a service that allows its users to store files on Dropbox's servers. According to Dropbox's privacy policy, at https://www.dropbox.com/privacy, Dropbox collects and stores "the files you upload, download, or access with the Dropbox Service," and also collects logs: "When you use the Service, we automatically record information from your Device, its software, and your activity using the Services. This may include the Device's Internet Protocol ("IP") address, browser type, the web page visited before you came to our website, information you search for on our website, locale preferences, identification numbers associated with your Devices, your mobile carrier, date and time stamps associated with transactions, system configuration information, metadata concerning your Files, and other interactions with the Service. "Dropbox is a free service that lets you bring all your photos, docs, and videos anywhere. This means that any file you save to your Dropbox will automatically save to all your computers, phones and even the Dropbox website."

CONCLUSION

124. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require each of the Providers to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

125. Based on the forgoing, I request that the Court issue the proposed search warrants.

REQUEST FOR SEALING

126. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

127. Pursuant to 18 U.S.C. § 2705(b) and for the reasons stated above, it is further requested that the Court issue Orders commanding each of the Providers not to notify any person (including the subscribers and customers of the accounts listed in the warrant) of the existence of the warrant until further order of the Court.

Respectfully submitted,

EVELINA ASLANYAN
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on June 23, 2017

Honorable Lois Bloom
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following accounts that is stored at premises controlled by the respective Providers, each of which is a company that accepts service of legal process in the United States.

Account Identifier	Provider
a@mediamethane.com	Google
a@mediamethane.com	LinkedIn
"adw0rd"	Atlassian
alex@adzos.com	Google
alex@tipsters.com	Google
assembla@betaggregator.com	Google
Dropbox User ID 94568916	Dropbox
Google Analytics Account 12145724	Google
[redacted]	Google
ibetters2@gmail.com	Google
loscritino@gmail.com	Google
"mathete"	Atlassian
"nastra"	Atlassian
qoqenator@gmail.com	Google
sergey@adzos.com	Google
support@adzos.com	Google

tech@clickandia.com	Google
x11org@gmail.com	Google

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all messages, chats and/or emails associated with the account, including stored or preserved copies of messages sent to and from the account, draft messages, the source and destination addresses associated with each message, the date and time at which each message was sent, and the size and length of each message;

b. The text of all Internet search requests input by the subscriber; and all URLs or IP addresses typed into the browser address bar or URLs or IP addresses clicked on;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All accounts associated with the account (including all accounts accessed by the brower(s) and device(s) associated with the account), as determined by an analysis of cookies and/or machine cookies;

e. The types of service utilized;

f. Any unique identifiers that would assist in identifying device(s) associated with the account, including push notification tokens associated with the account (including Apple Push Notification (APN), Google Cloud Messaging (GCM), Microsoft Push Notification Service (MPNS), Windows Push Notification Service (WNS), Amazon Device Messaging (ADM), and Baidu Cloud Push);

g. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, files, and postings;

h. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

i. With respect to Google Analytics Account 12145724, all analytics and tracking data associated with this account and all of its associated Tracking IDs; and

j. With respect to Google Analytics Account 12145724, all of the information specified in items a. through h. with respect to each associated Tracking ID.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1030(a)-(b) (computer fraud and conspiracy and attempt to commit the same), 1343 and 1349 (wire fraud and wire fraud conspiracy), those violations involving the user(s) of the account(s) listed in Attachment A, his/her co-conspirators, associates and others with whom he/she has communicated, and occurring between July 1, 2014 and June 23, 2017, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Committing computer fraud, wire fraud, or conspiring or attempting to commit any of the foregoing, including the creation and operation of botnets, and the committing of click fraud, digital video advertising fraud, and other types of advertising fraud;

(b) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the account about matters relating to computer fraud, wire fraud, and conspiracy or attempt to commit any of the foregoing, including records that help reveal their whereabouts.

JD:AFM
F. #2016R02228

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

17M561

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH AN ELECTRONIC ACCOUNT THAT IS STORED AT PREMISES CONTROLLED BY NAMECHEAP

TO BE FILED UNDER SEAL

No. _____

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, EVELINA ASLANYAN, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for an amended search warrant for information associated with certain accounts that is stored at premises controlled by Namecheap, Inc. ("Namecheap" or the "Provider"), an electronic provider headquartered in the United States. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Provider to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since March 2012. I am responsible for conducting and assisting in investigations

involving cybercrime. I have investigated and otherwise participated in numerous matters during the course of which I have conducted physical surveillance, interviewed witnesses, executed court-authorized search warrants and used other investigative techniques to secure relevant information. I am familiar with the facts and circumstances set forth below from my participation in the investigation, my review of the investigative file, and from reports of witnesses and other law enforcement officers involved in the investigation.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to search the information associated with a certain electronic account further described in Attachment A for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1030(a)-(b) (computer fraud and conspiracy and attempt to commit the same), 1343 and 1349 (wire fraud and wire fraud conspiracy), further described in Attachment B.

5. On June 23, 2017, Your Honor issued search warrants for information associated with certain email account and other electronic accounts. The affidavit submitted in support of the search warrants is attached hereto as Attachment C and is incorporated by reference herein. The search warrants that issued are attached hereto as Attachment D.

6. One of the accounts identified in Attachment C and Attachment D was the email account tech@clickandia.com. That account was identified in Attachment C and Attachment D as being hosted by Google. Upon further review of evidence gathered in the course of this

investigation, I discovered that this was an error, and that the account is in fact hosted by Namecheap.

7. Based on the foregoing, I respectfully request that the Court issue the proposed amended search warrant, which corrects the foregoing error.

8. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Evelina Aslanyan
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on June 26, 2017

HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the email account below that is stored at premises owned, maintained, controlled, or operated by Namecheap (the "Provider"), a company headquartered in San Francisco, California:

tech@clickandia.com

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all messages, chats and/or emails associated with the account, including stored or preserved copies of messages sent to and from the account, draft messages, the source and destination addresses associated with each message, the date and time at which each message was sent, and the size and length of each message;

b. The text of all Internet search requests input by the subscriber; and all URLs or IP addresses typed into the browser address bar or URLs or IP addresses clicked on;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All accounts associated with the account (including all accounts accessed by the brower(s) and device(s) associated with the account), as determined by an analysis of cookies and/or machine cookies;

e. The types of service utilized;

f. Any unique identifiers that would assist in identifying device(s) associated with the account, including push notification tokens associated with the account (including Apple Push Notification (APN), Google Cloud Messaging (GCM), Microsoft Push Notification Service (MPNS), Windows Push Notification Service (WNS), Amazon Device Messaging (ADM), and Baidu Cloud Push);

g. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, files, and postings; and

h. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1030(a)-(b) (computer fraud and conspiracy and attempt to commit the same), 1343 and 1349 (wire fraud and wire fraud conspiracy), those violations involving the user(s) of the account(s) listed in Attachment A, his/her co-conspirators, associates and others with whom he/she has communicated, and occurring between July 1, 2014 and June 23, 2017, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Committing computer fraud, wire fraud, or conspiring or attempting to commit any of the foregoing, including the creation and operation of botnets, and the committing of click fraud, digital video advertising fraud, and other types of advertising fraud;

(b) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the account about matters relating to computer fraud, wire fraud, and conspiracy or attempt to

commit any of the foregoing, including records that help reveal their whereabouts.

ATTACHMENT C

SK:AFM
F.#2016R02228

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH 12 EMAIL ACCOUNTS AND SIX OTHER ELECTRONIC ACCOUNTS THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, DROPBOX, LINKEDIN, AND ATLASSIAN	**TO BE FILED UNDER SEAL** **APPLICATION FOR SEARCH WARRANTS FOR INFORMATION IN POSSESSION OF PROVIDERS** Case No. 17-M-561

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANTS

I, EVELINA ASLANYAN, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for search warrants for information associated with certain accounts that is stored at premises controlled by Google, LinkedIn, Atlassian, and Dropbox (the "Providers"), electronic providers headquartered in the United States. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Providers to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since March 2012. I am responsible for conducting and assisting in investigations involving cybercrime. I have investigated and otherwise participated in numerous matters during the course of which I have conducted physical surveillance, interviewed witnesses, executed court-authorized search warrants and used other investigative techniques to secure relevant information. I am familiar with the facts and circumstances set forth below from my participation in the investigation, my review of the investigative file, and from reports of witnesses and other law enforcement officers involved in the investigation.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to search the information associated with certain electronic accounts and servers further described in Attachment A for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1030(a)-(b) (computer fraud and conspiracy and attempt to commit the same), 1343 and 1349 (wire fraud and wire fraud conspiracy), further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The FBI is investigating a massive and continuing fraud scheme known as "Metan," through which cybercriminals have siphoned away millions of dollars from U.S. companies.

7. The investigation so far has revealed that the scheme has been carried out in three stages, each of which has involved defrauding advertisers by creating the false impression that their online advertisements are being viewed or clicked on by human Internet users.

8. In the first stage, from approximately July 2014 to approximately September 2015, the conspirators used computers that they controlled to fraudulently click on advertisements and then took a share of the resulting revenue.

9. In the second stage, from approximately September 2015 to December 2016. the conspirators again defrauded advertisers. This time, the conspirators employed forged registration data to disguise their machines as the computers of real individuals browsing the Internet. They used these camouflaged machines, not to click on links, but to fabricate impressions of display ads[1] and video ads. They accomplished this by loading the advertisements on their own computers while sending falsified data up the commercial chain toward the advertisers, conveying the false impression that these non-existent Internet users were viewing the ads on premium websites. The conspirators pocketed the resulting

[1] "Display" advertisements, also known as banner advertisements, are online advertisements that typically consist of an image and associated text.

revenue. The second stage of the scheme ended when a cybersecurity firm publicly revealed the IP addresses of the computers that the conspirators were using to carry out the fraud, leading to those addresses' being blacklisted within the online advertising industry.

10. In the third stage, which began in or around November 2016 and is still being carried out, the conspirators are still committing display and video advertising fraud, but are doing so using third-party computers that are infected with malware.

11. The operators of the Metan system are mostly in Russia and the former Soviet Union, or are Russian expatriates living elsewhere. Where necessary, emails in Russian have been translated into English for purposes of this affidavit. These are draft translations.

a. Prior Search Warrant

12. On or about March 10, 2017, the Honorable Ramon E. Reyes, United States Magistrate Judge for the Eastern District of New York, signed search warrants authorizing the search of the following email accounts: adw0rds.yandex.ru@gmail.com, inno_rr@yahoo.com, ibetters@me.com, and mathete.com@gmail.com.

b. Background

(i) The Digital Advertising Market

13. Online services and websites are typically supported by advertisements. For example, while users of Google's search engine pay no fee to carry out web searches, Google charges advertisers to place advertisements among its search results. Similarly, users can browse many news and entertainment websites such as CNN.com for free because these sites charge advertisers to place advertisements on the sites. Within the online advertising industry, the term "publishers" is used to describe providers of content like Google or CNN. Broadly speaking, advertisers seek to place advertisements with publishers so that the ads can be seen and/or clicked on by human viewers who are drawn to the publishers' content.

14. Online advertisements can be divided into two categories. First, some advertisers rely on clickable links which, when clicked, bring the user to the advertiser's site. Advertisers typically pay each time such an ad is clicked on, a pricing model known as "cost per click" or "CPC." By contrast, other advertisers rely on content (such as images or videos) which appears in an allocated space within a webpage so that users encounter it in the midst of browsing. Because such content does not need to be clicked on to make an impact on viewers, the advertiser does not pay only for clicks, but instead pays every time a user loads a page on which the ad has been placed—a pricing model known as "cost per thousand impressions" or "CPM."

15. Publishers obtain ads from advertisers (via a long chain of intermediaries) using a short string of computer code called an "ad tag" that is embedded in the code making

up the publisher's web page.[2] The ad tag does not itself contain an ad; rather, it triggers the process that determines what advertisement will be shown in a designated spot on the page. The ad tag is furnished by an entity called an ad network that serves as an intermediary between the publisher and the pool of potential advertisers.

16. When a user loads a webpage, and the user's web browser encounters an ad tag, there ensues a split-second auction in which multiple advertisers bid for the opportunity to show an ad to that particular user on that particular web page. Agents for potential advertisers receive information that includes the user's internet service provider; his or her IP address; and the website that he or she was visiting when he or she clicked the link that led to the request to load the ad. This last piece of information, known as the "referer," is crucial because the identity of the website last visited by the user sends a signal about the user's value and also may correlate with the user's destination, where the ad will ultimately be shown.[3] The referer's identity is conveyed by the user's computer in a short message known as a "referer header."

17. When an advertiser "wins" this auction, its ad is uploaded from a separate computer (known as an "ad server") into the spot on the web page indicated by the ad tag. All of this takes place in microseconds, without the awareness of the user who is loading the

---

[2] In practice, the publisher may instead incorporate a "frame" into which a shifting series of ad tag code may be uploaded without the publisher's intervention.

[3] For instance, a user whose referer-header indicates that he has just visited CNN.com may well be headed toward a sub-page of CNN, such as CNN.com/domestic.

web page. The advertiser then pays the various intermediaries involved, as well as the publisher.

18. On any given web page, there may be multiple pieces of advertising "real estate" to be filled in this way. A website whose advertising real estate is highly desirable may be able to fill all of its ad slots in these split-second auctions (known as a "100% fill"). A website whose real estate is less desirable may achieve a lower rate of "fill."

19. An ad network has an incentive to place its ad tag on as many websites as possible to maximize revenues. In order to achieve this, the ad network may contract with another ad network (known as an "extended ad network") that has its own relationships with publishers. The extended ad network agrees to place the primary network's ad tag on the websites of the extended network's affiliated publishers, in return for a share of the resultant revenue.

(ii) The Fraudulent Schemes

20. Based on my review of the evidence in the investigation so far, including email records, network traffic information, subscriber information from online services, and information from cybersecurity researchers, the Metan conspirators have perpetrated an advertising fraud scheme that has taken several different forms over the past few years.

21. As set forth below, the instant scheme began as click fraud (the "Click Fraud Scheme"). In click fraud, malicious actors make money by directing computers they control to click on advertisements that have been placed on a cost-per-click basis. The advertisers then receive all or a share of the payments for these clicks.

22. With time, though, the scheme evolved to a new effort to defraud advertisers through fraudulent impressions of display and video advertisements (the "Display/Video Ad Fraud Scheme"). In this second scheme, rather than clicking on CPC ads, the fraudulent traffic directed by the conspirators would load, and purport to view or play, CPM ads. The conspirators referred to these schemes (both the Click Fraud Scheme and the Display/Video Ad Fraud Scheme) as "*Metan*," the Russian word for "Methane," As a front for their activities, the conspirators used Mediamethane, an ad network owned by Alexander Zhukov.

23. In preparation for the Display/Video Ad Fraud Scheme, the Metan conspirators acquired approximately 500,000 IP addresses, for which they created false registration information so that the addresses appeared to belong to real Internet users. A cybersecurity firm gathered the information documenting these false registrations, and I have reviewed a sample of that documentation.

24. The conspirators posed as an extended ad network to gather ad tags belonging to both complicit and unsuspecting ad networks. The conspirators then used the IP addresses they controlled to load these ad tags in such a way as to make it falsely appear to advertisers that the ad tags were being launched under circumstances justifying a high bid on the ads, when in fact the ads were not being seen by anyone. They did so, first, by sending false referer headers indicating that these hundreds of thousands of simulated Internet users were requesting the advertisers' ads after having visited websites such as nfl.com and oprah.com.[4]

---

[4] As noted above, a user who has just visited a high-value website is of value both because he is likely to visit other such websites and because, in practice, most online clicks that are placed on a high-value website only serve to move the user deeper into that same website, as

Having won the auctions, the conspirators then sent fraudulent requests to relevant ad servers that reinforced the appearance the ads were being served to these high-value websites.

25. The Display/Video Ad Fraud Scheme ended in December 2016, when the cybersecurity firm White Ops published a list of the IP addresses involved.

26. In or around November 2016, however, the Metan conspirators appear to have begun a new scheme—the "Hybrid Scheme"—that engaged in display and video ad fraud using a refinement of the conspirators' earlier technology.

27. The Hybrid Scheme resembles the previous schemes in that video and display ads are again being accessed by bots. However, the Hybrid Scheme employs victim computers that have been infected with malware, allowing the conspirators to funnel fraudulent traffic through them.

28. With regard to all of their schemes, the conspirators took measures to circumvent the third-party fraud detection services that many advertisers use to verify that they are not paying for fraudulent traffic. When a video ad is played on the computer of a putative Internet user, sophisticated verification software often scrutinizes the computer viewing the ad to ensure that it bears some indicia of human use. For example, based on statistical patterns of Internet usage, vendors of verification software expect to see that a certain percentage of viewers of an advertisement are also using Facebook at the same time. The conspirators took steps to ensure that the requisite percentage of the phantom "users"

---

when a browser on nytimes.com moves from one article to another. Thus, the referer-header, while it nominally conveys information only about the origins of an Internet user, also tells a story about the user's likely destination.

viewing the ads would show signs of Facebook use. Similarly, because traffic that originates only in the United States is a red flag that the traffic is of fraudulent origin, the conspirators sought to ensure that the supposed Internet users visiting the advertisements appeared to come from a number of countries. The conspirators also worked with co-conspirators at complicit ad networks to selectively block the anti-fraud code from loading in such a way that the verification companies would not be aware that their detection software had been evaded.

29. The investigation so far has revealed the following central players in the Click Fraud, Display/Video Ad Fraud, and Hybrid Schemes:

- **Alexander Zhukov** directed the Click Fraud and Display/Video Ad Fraud schemes and served as the CEO of Mediamethane, an associated company that posed as an extended ad network. Zhukov was in charge of the Metan team's relationships and communications with third parties, including co-conspirators.
- **Boris Timokhin** served as the chief programmer for the scheme.
- **Mikhail Andreev** provided early programming assistance in developing the Click Fraud Scheme.
- **Dmtri Novikov** provided early programming assistance in developing the Click Fraud Scheme.
- **Denis Avdeev** participated in the Click Fraud and Display/Video Ad Fraud Schemes and appears to have served as a technical liaison to network administrators at other companies.
- **Sergey Ovsyannikov** operated AdZos and Clickandia, entities that engaged in the Click Fraud, Display/Video Ad Fraud, and Hybrid Schemes.

c. The Click Fraud Scheme

30. Evidence indicates that the development of the Click Fraud Scheme began during the summer of 2014.

31. On or about July 17, 2014, Boris Timokhin ("Timokhin")[5] sent emails to Mikhail Andreev (using the email account x11org@gmail.com), Dmitry Novikov (using the email account whitelotusoflove@yandex.ru), and an unknown individual identified only as "Alexey." The emails contained a formal document outlining the ground rules for a "partnership" whose purpose was not described, but which would include conversion of funds into cryptocurrencies as necessary. The venture described in the document was to use a company called VBBB, which is known through open sources to be associated with Alexander Zhukov ("Zhukov").

32. Thereafter, as set forth below, numerous emails regarding click fraud were exchanged between Timokhin, Andreev, Novikov, and Zhukov.

33. The conspirators were assisted by two outside [redacted]. Both entities appear to have coached the conspirators in how to make the Metan botnet's fraudulent clicks appear to be human-generated.

---

[5] Unless otherwise specified, for all emails discussed in this affidavit, Timokhin used the email address mathete.com@gmail.com.

(i) Contribution of Clickandia to the Click Fraud Scheme

34. For example, on or about October 22, 2014, Dmitri Novikov wrote a posting in an internal communications group used by the conspirators to track progress on the click fraud project, within a project-tracking tool called Jira.

35. Jira is a product of the Atlassian Corporation. Users of Jira, and of a related Atlassian product called Confluence, are assigned usernames which may be used to store some of their message content in servers maintained by Atlassian. Messages created using these tools and found in the conspirators' email accounts, indicate that Andreev's Atlassian username was "Adw0rd"; Zhukov's username was "Nastra"; Novikov's usernames were "Listentome" and "Legefix"; and Timokhn's username was "Mathete." Messages sent through Jira and Confluence among the conspirators generally originated in a single email address (that appears to have been shared among the conspirators): assembla@betaggregator.com. From there, the messages were emailed out to the other conspirators.

36. Novikov's posting quoted a message he had apparently received from an email address called "tech@clickandia.net." As quoted in Novikov's posting, the Clickandia contact had stated: "you don't have 'accept' language in your headers while clicking. We don't have this kind of verification anymore, but a lot of providers have it. Hence accept-language for a search and a click must be identical." Novikov annotated this feedback as follows: "you need to add accept-language to a header while clicking."

37. Based on my training and experience, in these exchanges, Clickandia was giving the Metan conspirators advice on how to make the botnet's clicks look more like

human clicks. Specifically, the message from Clickandia indicated that many ad networks would only accept a click as valid if the browser that was carrying out the click emitted a short string of text (known as the "accept-language header") indicating the putative user's preferred language. If the Internet users simulated by Metan did not provide this information, their clicks would not register as real.

38. Another relevant exchange occurred on or about November 13, 2014, when Novikov updated a Confluence status tracker that was laid out in the form of a grid. In the row marked "Clickandia," in a column marked "Current issues," Novikov inserted the comment "Discussing mouse move." In a column marked "Click status," Novikov deleted the words "Not Clicking" and added "working."

39. Based on my training and experience, both of these comments relate to further refinements that the Metan team was making so that the clicks emanating from their botnet would appear to be coming from human Internet users. The note about "mouse move" related to an effort to remotely induce mouse movements in the computers that were clicking on Clickandia's links, so as to deceive advertisers' fraud-detection software by creating the illusion that there were humans at the controls of these computers. The change to "click status" meant that the bots' clicks on Clickandia's links were now being registered, as required to generate revenue.

40. Clickandia also appears to have been involved in video ad fraud. On or about October 28, 2014, Novikov wrote a message to Timokhin using Jira with the subject line "Emulating 'the viewing of a video.'" Novikov provided the URL "mycoolwebsite.net" and wrote, "Boris: Here [is where] Clickanda measures video."

41. Mikhail Andreev (who was one of the recipients of Timokhin's July 17, 2014 contract) appears to have provided technical assistance to the Metan team in bypassing the third-party verification vendors who were vetting Clickandia's traffic. On or about November 27, 2014, Andreev wrote a note in Confluence, providing computer code "to bypass their filter."

42. On or about May 8, 2015, Andreev used the email address x11org@gmail.com to send Timokhin an email entitled "USD account." The email contained United States correspondent banking account information for an account in Andreev's name at the Russian bank Alfabank.

(ii) Contribution of Affiliate Harbour to the Click Fraud Scheme

43. Crucial assistance in the development of the Click Fraud Scheme was also provided by [redacted], which appears to have commissioned the Metan botnet to click on ads belonging to [redacted], and also to have provided extensive technical support toward that goal.

44. For example, in a to-do list that Zhukov (using his ibetters2@gmail.com email account) sent to Timokhin on or about June 25, 2015, Zhukov made frequent reference to the complaints and demands of [redacted] and other partners.

45. In one item, Zhukov directed Timokhin "to find [the] [redacted] checker and see why they are complaining." Zhukov said that [redacted] had complained about a lack of "mouse move," and passed on some computer code that he said [redacted] had "given for friendship's sake."

46. Zhukov also noted that another entity had complained about "fake Chrome and mouse move."

47. Based on my training and experience, Zhukov was passing on a request from [redacted] that Timokhin locate and neutralize a piece of third-party software intended to identify fraudulent web traffic (known as a "checker" or "pixel"), because the software was leading to the denial of payment for the botnet's clicks on advertisements placed by [redacted], thus depriving both [redacted] and Metan of revenue. [redacted] had advised Zhukov that the software was detecting a lack of "mouse move," i.e. human-seeming mouse movements, and Zhukov noted that another partner had complained about detecting "fake Chrome," meaning that the clicks did not come from full-fledged Chrome web browsers such as a human browsing the Internet would use, but rather from simulated browser software operating on bots which were not truly viewing the ads in question. Zhukov indicated that "for friendship's sake," [redacted] had passed along tips for drafting computer code to resolve some of these problems.

48. Finally, in another item in the same list, Zhukov asked Timokhin "to add authorization for Facebook [] users. There is Google, twitter too; [but] no FB (There should be approximately 40% of them.)" Based on my training and experience, Zhukov was telling Timokhin that in order for the bots' clicks to appear real to fraud detection firms, at least 40% of the computers in the network had to appear to be signed into Facebook. Zhukov also indicated that this effort had already been undertaken with respect to Twitter and Google.

49. Numerous other emails reflect the efforts of [redacted] to assist the Metan conspirators with the click fraud scheme. For example, on or about June 29, 2015,

Zhukov (using his ibetters2@gmail.com account) emailed Timokhin an exchange that Zhukov had had with [redacted] in which [redacted] wrote: "Let's try to understand why the bot flies by the detection URLs… you need to understand that you cannot bypass the most simple of filters when the URL that you switch to changes." Based on my training and experience, in this exchange [redacted] was helping Zhukov to redesign Metan so that it could "bypass," or evade, the various third-party programs or "filters" designed to detect nonhuman traffic.

d. Zhukov Forges Internet Pedigrees for Metan's Simulated Internet Users

50. As discussed above, a key element of both the Click Fraud and Display/Video Ad Fraud Schemes was that real Internet users had to appear to be clicking on or viewing the ads, when in fact the ads were being clicked on by Metan's bots (in the case of the Click Fraud Scheme) or viewed and played by the bots (in the case of the Display/Video Ad Fraud Scheme). Moreover, high-value characteristics were chosen for these non-existent users so that they would command a high price from ad networks. To accomplish this, the conspirators disguised the internet service providers to which their supposed Internet users subscribed.

51. The conspirators accomplished this with the aid of IP address leasing companies which had the ability to modify entries in a worldwide directory attributing IP addresses to companies.

52. For example, on or about April 24, 2016, Zhukov (using the email address alex@tipsters.com) forwarded Timokhin an email exchange that Zhukov had engaged in with a representative of an IP address leasing company.

53. In that exchange, the leasing company confirmed false directory information provided by Zhukov that incorrectly listed [redacted] as the controller of an IP address when, in fact, it was Zhukov who controlled the IP address.

54. Based on my training and experience, the effect of this false directory entry, in combination with the many other false entries that the conspirators created, was to create the impression that the simulated Internet users clicking on links or viewing display and video ads were a disparate group of real individuals, many connecting to the Internet as customers of Internet service providers that showed them to be high-value viewers. If the advertisers had been aware of the reality that the machines "watching" the ads were accessing the Internet from a block of IP addresses that was under common control, this would have served as a clear tipoff that the clicks and ad impressions were fraudulent and therefore worthless.

e. The Display/Video Ad Fraud Scheme

55. Approximately during the summer of 2015, the Metan conspirators began to develop the Display/Video Ad Fraud Scheme. Rather than profit from fraudulent clicks, the Metan conspirators would heretofore seek to generate fraudulent views, meaning that they would deceive advertisers into thinking that their ads had been viewed by humans, when in fact they had not. Individual instances in which an ad is viewed by an Internet user are known in the industry as "impressions."

56. In order to "view" display ads and "play" video advertisements, the conspirators made use of the disguised IP addresses they controlled.

57. However, in a departure from the click fraud scheme, Metan's phantom Internet users did not actually travel around the web to commit display and video ad fraud.

Rather, each of the Metan bots simply transmitted a referer header that (falsely) indicated that it had just visited a high-value website, touching off the split-second auction discussed above. The Metan system then transmitted a message to the appropriate ad server that purported to download the ad to a page on that high-value website, cementing the false impression that a user was browsing the site. In fact, the page to which the ad server transmitted the ad was a forgery that resided on Metan's servers, and not on the high-value website.

58. An email from Zhukov (using ibetters2@gmail.com) to Timokhin, dated October 17, 2016, displays the Metan team's attempts to refine both elements of this scheme—the non-existent high-value users and the forged high-value websites—using feedback from [redacted], a co-conspirator [redacted] further discussed below whose name the conspirators sometimes abbreviated as [redacted]

59. Zhukov commented to Timokhin that "We agreed with [redacted] – 75%. Additionally, they are helping." He added: "They made a note that the traffic is 100% US. This immediately strikes the Buyer as a sign that it's a bot. The second sign: Equal domain distribution 5% 5% 5%. It needs to be totally random."

60. Based on my training and experience, this email lays out the rough financial terms of Metan's relationship with [redacted] and also passes on [redacted]'s suggested refinements to the scheme. First, Zhukov commented that [redacted] would be giving Metan its ad tags so that Metan could create fraudulent ad impressions against ads provided by [redacted] clients. In return, [redacted] would give the Metan team 25% of the resultant revenue while keeping 75% for itself.

61. Second, Zhukov related two areas in which the Display/Video Ad Fraud Scheme must improve. First, the phantom Internet users simulated by Metan must appear to hail from a range of countries, rather than being "100% US." Second, the browsing habits of these nonexistent Internet users should be realistically "random," rather than segmented among websites in rigidly fixed percentages ("5% 5% 5%").

(i) The Metan Team Accepts Orders for Referers

62. As discussed, the conspirators were deceiving advertisers (and other players in the Internet advertising ecosystem) into believing that ads were being viewed on real websites. Websites that are both highly trafficked and high "fill" generate more advertising revenue than poorly trafficked, low-fill sites, since the advertising real estate on such websites is both expensive and densely occupied.

63. The Metan conspirators sought to fabricate high-value referers for their non-existent Internet users. Moreover, they customized these fraudulent website lists at the request of the different ad networks they conspired with, in an effort to simulate, for each ad network, the websites which would give that network the highest "fill."

64. Many of the telltale communications underlying this scheme involve an ad network providing the Metan conspirators with (1) an ad tag (to permit the uploading of ad content) and (2) a long list of high-fill websites.

65. Based on my knowledge, training, and experience, and consultation with individuals in the advertising industry, in legitimate commerce, an extended ad network can only place ads with publishers with whom it has a relationship. Thus, before requesting placement from an extended ad network, the requesting network would have to first inquire

about the extended network's portfolio of relationships, and tailor its request accordingly. But the Metan team's communications with ad networks did not fit this model. Rather, and tellingly, the Metan team appeared able to accept unrestricted requests from Mediamethane's partners for ad placement, without limitations as to publisher.

66. For example, on or about October 18, 2016, Zhukov (using his a@mediamethane.com email account) exchanged emails with an individual named [redacted] who used the email address [redacted].

67. In an email with the subject line "Business Partnership," [redacted] introduced himself and then sent Zhukov an ad tag, along with a lengthy list of high-traffic websites (such as [redacted].com, [redacted].com, [redacted].com, and [redacted].com). [redacted] wrote to Zhukov: "Please find the high filling domains across the different platforms we use. See if you have access to these domains and drive more traffic."

68. Based on my training and experience, this instruction would not be given in a legitimate business context because an extended ad network that lacked Metan's ability to forge ad placement would not simply "have access" to the domains on an extensive list of high-traffic websites.

69. Other communications with external partners similarly indicate that the Metan team was unconstrained by normal technical and business limitations. For example, on or about June 23, 2015, Zhukov (using his ibetters2@gmail.com email account) received an email from an individual named [redacted], who used the email address [redacted]. [redacted]f provided an ad tag and cautioned Zhukov as follows:

"Here is the new feed as I promised. Please limit it to around 3mil searches per day for now."

70. Based on my training and experience, in this communication, [redacted] was reversing the normal business logic of the advertising industry. Rather than asking Zhukov to *maximize* traffic, [redacted] was asking Zhukov to *limit* the traffic on [redacted]'s ad tag—an instruction that would only make commercial sense in an environment where Zhukov was able to direct unlimited amounts of Internet traffic to websites of his choosing, to an extent that might have caused technical difficulties or raised the concern of traffic verification companies.

71. Evidence from the execution of prior search warrants indicates that the Metan conspirators corresponded with [redacted] employees from June 23, 2015 to November 24, 2015.

(ii) Zhukov Accepts Orders From [redacted] For Websites to Run Ads On

72. In addition to taking orders from companies like [redacted] and [redacted], the Metan conspirators also worked on a partnership basis with some ad networks that not only solicited fraudulent Internet traffic, but also provided crucial assistance in refining Metan's fraud technology. Among these was a company called [redacted].

73. For example, on or about October 13, 2016, Zhukov (using the email address a@mediamethane.com) emailed [redacted], a [redacted] employee whose email address is [redacted]. Zhukov wrote, "Send me please fresh top 20 refers domain for USA prerolls."

74. [redacted] responded, "Here [are] the top USA desktop domains nowadays," along with a list of major websites, such as [redacted], and others.

75. Zhukov, again using his Mediamethane email account, then forwarded [redacted]'s email to Timokhin, commenting, "Add please fresh refers in place of the old ones for [redacted] Timokhin responded: "DONE."

76. Based on my training and experience, in this exchange Zhukov solicited from [redacted] a newly updated (or "fresh") list of the websites (or "refers") with the highest fill and/or traffic at that moment. [redacted] then sent the requested list to Zhukov, and Zhukov in turn asked Timokhin to fraudulently create the appearance that users were visiting these websites and watching ads on them, in place of a prior list of websites ("the old ones").

77. A similar exchange occurred on October 14, 2016, when Zhukov (using his ibetters2@gmail.com email account) forwarded Timokhin a similar list of prominent websites with the subject line "Top 30 from [redacted] and the note "Can be replaced." When Zhukov thanked Timokhin for adding these sites, Timokhin wrote, "We are doing it for the money." In apparent agreement, Zhukov responded: "Glory to having balls… In the end, cash conquered evil."

78. Based on my training and experience, in this exchange Zhukov was replacing the prior list of high-fill websites with a newly updated list provided by [redacted] ([redacted]). When Zhukov thanked Timokhin for implementing the change, Timokhin pointed out that these thanks were unnecessary, since they were both out to make money.

79. Similarly, on October 27, 2016, Zhukov (using his a@mediamethane email address) forwarded to Timokhin an email that he had received from an individual using the

name [redacted] and the email address [redacted]. [redacted] sent Zhukov a list of web domains with the preface: "Bro… Any way you can change to run these sites please," which Zhukov passed on to Timokhin, noting, "Add new referres to the [redacted] please."

80. Based on my training and experience, "[redacted] is an abbreviation for "[redacted]," indicating that [redacted] worked at [redacted].

81. On or about October 16, 2016, Zhukov used his ibetters2@gmail.com account to forward Timokhin another communication that demonstrated the degree of assistance [redacted] was supplying to the Metan conspirators.

82. In the forwarded communication, which was a log of an online chat, Zhukov was conversing with an individual identifying himself as "[redacted]."

83. In the exchange, "[redacted]" and Zhukov (identified as "Aleksandr Zh") discussed "checks" using "Fraudlogix" and "MOAT" and "IAS," and Zhukov queried whether he needed to "get [a] report… to see where we have to make fixes." [redacted] responded: "I checked today and nothing… shows no alerts."

84. Zhukov transmitted this exchange to Timokhin with the subject "a moment of vanity." Zhukov then added the prefatory comment, "Metan is magnificent" and the following postscript: "Made friends with the [redacted].. he understands what kind of solution we have and he wants to work, and he is ready to cooperate[.]"

85. Based on my training and experience, in this exchange [redacted] (using the nickname "[redacted]") was helping Zhukov to evade various fraud detection services to which [redacted] had access, including those provided by Fraudlogix, Moat, and Integral

Ad Science ("IAS"). [redacted]t was reassuring Zhukov that the simulated traffic created by Metan was not running afoul of any of these services' fraud detection filters ("no alerts"). Zhukov, in turn, was excitedly relaying this result to Timokhin ("Metan is magnificent") and was also pointing out to Timokhin that [redacted] was fully colluding with Metan ("he is ready to cooperate").

86. The Metan co-conspirators appear to have advertised for partners and/or co-conspirators on LinkedIn, based on an email that Zhukov received on October 26, 2016 from a potential partner that began as follows: "We saw your posting on Linkedin." Zhukov received the email at his a@mediamethane.com email address, indicating that Zhukov used this address as the registration email for his LinkedIn account. Zhukov subsequently appears to have generated fraudulent ad traffic on behalf of the individual who contacted him via LinkedIn.

(iii) The Metan Conspirators Create Fraudulent Traffic for [redacted]

87. In addition to [redacted], the conspirators received orders for fraudulent Internet traffic from an advertising network they referred to as "[redacted]

88. [redacted] had apparently struck a deal whereby ads would be placed only on webpages that also bore certain keywords. Thus, in order to assist [redacted] in defrauding [redacted]'s advertiser clients, the Metan conspirators had to create specialized fraudulent pages with the necessary keywords for the bots to "visit."

89. On or about October 13, 2016, in an email with the subject line "new domains for feeds with filled in titles and keywords," Timokhin emailed Zhukov at his ibetters2@gmail.com account as follows: "It is my understanding that new domains were

sent for [redacted] But his feed has keywords. I.e., if there are no pages for the domain here - https://centbycent.com/meth/prerolls/prerollvideopage/, then we don't fill the feed at all and most likely, we get zero fill for this domain. In such cases, I send the domains to [redacted] and he puts the pages together and then I add them."

90. Based on my training and experience, Timokhin was outlining his plan for dealing with [redacted] need for keywords: Timokhin would have "[redacted] create false pages ("put[] the pages together") with the requisite keywords.

91. Later that same day, Zhukov (using his ibetters2@gmail.com address) emailed Timokhin a link to an image file that was stored on the Dropbox file storage service, at a URL that (based on information reported by Dropbox) is associated with Dropbox User ID [redacted]

92. Timokhin responded, "Everything got kinda worse in the past hours[.] Maybe we should go back to the… old domains with the keywords? Meanwhile, [redacted] will collect [keywords] today-tomorrow for the new pages?"

93. Zhukov wrote, "Let's cut them off completely for now… let them freak out a bit… and tomorrow, we will start with a clean slate." Timokhin responded: "I am cutting [redacted] off completely, and giving [redacted] the domains to get the keywords in there."

94. Based on my training and experience, in this exchange, Zhukov was conveying to Timokhin that their attempt to craft keyword-laden pages to help [redacted] had been unsuccessful. The image file that Zhukov sent Timokhin was most likely a screen capture showing a control panel with performance statistics for the Metan fraud. The solution that the Metan conspirators arrived at was to temporarily cease providing fraudulent

traffic for [redacted] and to use the interval to have Avdeev create fresh domains with new keywords.

95. Information obtained from Dropbox indicates that Zhukov controls the Dropbox account with User ID [redacted] The registered user of the account has email account i-betters@ya.ru, and goes by the name Alexander Zhuk.

f. **The Metan Conspirators Develop the Hybrid Scheme**

96. In December 2016, the cybersecurity firm [redacted] published a white paper revealing the Metan scheme (which [redacted] termed "Methbot") and disclosing the IP addresses that the Metan conspirators were using. In response, those IP addresses were blacklisted by cybersecurity firms, effectively ending the Display/Video Ad Fraud Scheme.

97. At the same time, however, the conspirators, or individuals who were associated with or learned from the conspirators, appear to have been developing a new scheme (the "Hybrid Scheme") that made use of victim's computers that had been infected with malware to load display and video ads for fraudulent purposes.

(i) The Hybrid Scheme is Linked to Adzos.com and Clickandia.com

98. The Hybrid Scheme was observed in or around April 2017 by the advertising infrastructure provider [redacted] discovered that when certain video ads were loaded, attempts were apparently being made to block fraud detection software. Upon further investigation, [redacted] determined that the affected advertisements had one thing in common: connections to an extended ad network called AdZos.

99. [redacted] gives its customers the ability to log in to a proprietary portal where they can monitor ad performance. [redacted]s customers use their email addresses as login

usernames. The [redacted] clients affiliated with AdZos were found to have supplied the email addresses support@adzos.com and sergey@adzos.com as usernames.

100. Information reported pursuant to a subpoena by the internet service provider Digital Ocean indicates that a user with the email address sergey@adzos.com has repeatedly signed into Digital Ocean from an IP address associated with AdZos and has, in the course of paying Digital Ocean's invoices, identified himself as Sergey Ovsyannikov.

101. AdZos appears to be under common control with Clickandia, the ad network whose operators assisted the Metan team in setting up their click fraud operation. According to Digital Ocean, Ovsyannikov also pays the bills for Clickandia.com. Moreover, the AdZos and Clickandia websites are identically designed in terms of graphics, formatting, and images, albeit with different text.

102. Logs of data traffic associated with the Hybrid Scheme contain identifiers that have also led investigators back to AdZos. These logs, assembled by the cybersecurity firm [redacted], show that the malicious actors appear to have been tracking their performance using Google Analytics, a website traffic analysis tool operated by Google.

103. Google Analytics users are assigned a "Tracking ID" for use in tracking the performance of online elements. A Tracking ID consists of the letters "UA," followed by a hyphen, followed by the user's Google Analytics account number, followed by a hyphen and a "property number" denoting the particular element being tracked.

104. The string UA-12145724-11 appears in the logs of malicious traffic.

105. Information provided by Google indicates that among the registered users of that Tracking ID are individuals with email addresses sergey@adzos.com and alex@adzos.com.

(ii) The Hybrid Scheme is Linked to Loscritino@gmail.com

106. In addition to the Adzos.com email accounts described above, Google has reported that Tracking ID UA-12145724-11 is associated with another relevant email account, loscritino@gmail.com, as well as a relevant web domain, mycoolwebsite.net. Each of these identifiers is associated with other elements of the fraud under investigation. Mycoolwebsite.net was identified by Dmitri Novikov in October 2014 as a site connected to Clickandia's efforts "to emulate 'the viewing of a video.'" See supra ¶ 40. A user with the username "loscritino" registered the domain names for both Mycoolwebsite.net and Clickandia.com, according to the domain name registrar Namecheap.

(iii) The Fraud Scheme is Linked to Qoqenator@gmail.com

107. According to information provided by Google, the email account qoqenator@gmail.com belongs to Timokhin. On or about October 2, 2014, Zhukov (using his a@vbbb.com email account) forwarded to qoqenator@gmail.com an email that Zhukov had received the previous day from Mikhail Andreev's email account, x11org@gmail.com. The email bore the subject "Fwd: urls" and included various website addresses, including mycoolwebsite.net, the website address linked to Google Analytics Tracking ID UA-12145724-11. Qoqenator@gmail.com is also the "recovery account" for Timokhin's email account mathete.com@gmail.com (used throughout the fraudulent schemes), meaning that

Timokhin registered qoqenator@gmail.com as the email address at which he wished to receive emails if the "mathete" account became inaccessible.

THE TARGET ACCOUNTS

108. This search warrant seeks authorization to search the following premises for the period July 1, 2014 to June 23, 2017.

a. Email Accounts:

i. **a@mediamethane.com**, hosted by Google, was the Mediamethane email address used by Alexander Zhukov, who appears to have directed the Click Fraud and Display/Video Ad Fraud Schemes. Zhukov often used this email address to communicate about the Metan schemes with co-conspirators at other businesses, including [redacted] Zhukov also received a message at this email address responding to a LinkedIn posting he had created seeking potential business partners.

ii. **alex@adzos.com,** hosted by Google, is one of the registered email accounts for Google Analytics Tracking ID UA-12145724-11, which appears in data traffic related to the Hybrid Scheme. Based on my knowledge, training, and experience, and my review of the workings of Google Analytics, individuals using Google Analytics receive real-time emails at their registered email accounts regarding performance of the website being tracked, revenue flow, traffic characteristics, other email addresses associated with the website, and changes in service to the account.

iii. **alex@tipsters.com**, hosted by Google, was used by Alexander Zhukov. Zhukov used this email address on or about April 24, 2016 to communicate about leasing an IP address with false registration information.

iv. **assembla@betaggregator.com**, hosted by Google, appears to have been a central "hub" email address that was used to centrally receive, and then retransmit to all the conspirators, updates made by the conspirators to their Jira or Confluence workflows

v. [redacted] hosted by Google, was used by [redacted] at [redacted] to communicate with the Metan conspirators about domain names to be used in the Display/Video Ad Fraud Scheme. In a non-email chat, [redacted] also

gave the Metan conspirators technical advice about defeating fraud detection systems.

vi. **ibetters2@gmail.com**, hosted by Google, was frequently used by Alexander Zhukov through the course of the fraudulent schemes for communications with his co-conspirators regarding the scheme.

vii. **loscritino@gmail.com**, hosted by Google, is one of the registered email accounts for Google Analytics Tracking ID UA-12145724-11, which appears in logs of recent malicious traffic associated with the Hybrid Scheme. In addition, the username "loscritino" was used to log in to the domain registrar Namecheap in order to register the websites Clickandia.com and mycoolwebsite.net As described above, the registered email account for a Google Analytics account typically receives real-time emails at their registered email accounts regarding performance of the website being tracked, revenue flow, traffic characteristics, other email addresses associated with the website, and changes in service to the account.

viii. **qoqenator@gmail.com**, hosted by Google, was used by Boris Timokhin and received an email regarding the fraudulent scheme from Zhukov. This email account is the "recovery account" for Timokhin's email account mathete.com@gmail.com (used throughout the fraudulent schemes), meaning that Timokhin registered qoqenator@gmail.com as the email address at which he wished to receive emails if the "mathete" account became inaccessible.

ix. **sergey@adzos.com**, hosted by Google, is the email of record for the website of the ad network AdZos, associated with video streams recently observed to have blocked antifraud software. This email account is one of the registered email accounts for Google Analytics Tracking ID UA-12145724-11, which appears in data traffic related to the Hybrid Scheme.

x. **support@adzos.com,** hosted by Google, is one of the email addresses used by AdZos employees to log into LKQD's online portal.

xi. **tech@clickandia.com** is an email address that corresponded frequently with the Metan conspirators regarding the Click Fraud scheme.

xii. **x11org@gmail.com** was used by Mikhail Andreev to communicate with the other Metan conspirators regarding the fraudulent schemes under investigation.

b. Other Premises:

i. **Atlassian username "Adw0rd**," a username in Confluence and Jira project-tracking software hosted by the Atlassian Corporation, was

used by Mikhail Andreev to communicate with the other Metan conspirators regarding the fraudulent schemes under investigation.

ii. **Atlassian username "Mathete,"** a username in Confluence and Jira project-tracking software hosted by the Atlassian Corporation, was used by Boris Timokhin to communicate with the other Metan conspirators regarding the fraudulent schemes under investigation.

iii. **Atlassian username "Nastra,"** a username in Confluence and Jira project-tracking software hosted by the Atlassian Corporation, was used by Alexander Zhukov to communicate with the other Metan conspirators regarding the fraudulent schemes under investigation.

iv. **Dropbox account with User ID 94568916** was used to host an image containing performance metrics for the Metan botnet and is registered to Alexander Zhukov.

v. **Google Analytics Account 12145724** was used to track the performance of the Hybrid Scheme. An associated Tracking ID, 12145724-11, is specifically associated with mycoolwebsite.net. a site that appears to have been used by Clickandia in connection with video ad fraud.

vi. **LinkedIn account registered to a@mediamethane.com**: Alexander Zhukov appears to have advertised for partners and/or co-conspirators using this LinkedIn account. The Metan botnet generated apparently fraudulent display/video ad traffic on behalf of a contact who first reached out to Zhukov via this LinkedIn account.

Therefore, based on my knowledge, training, and experience, and the facts set forth in this affidavit, there is probable cause to believe that each of the aforementioned premises contains evidence of the crimes under investigation.

BACKGROUND CONCERNING EMAIL

109. In my training and experience, I have learned that each of the Providers provides a variety of on-line services, including electronic mail ("email") access, to the public. Each of the Providers allows subscribers to obtain email accounts at certain domain names, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with the Providers. During the registration process, each of the Providers asks

subscribers to provide basic personal information. Therefore, the computers of the Providers are likely to contain stored electronic communications (including retrieved and unretrieved email for the Providers' subscribers) and information concerning subscribers and their use of the Providers' services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

110. A subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by the Providers. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

111. In addition, I am aware that providers offer services through which a computer user can search webpages for text that the user types in, and that under some circumstances the provider saves the user's text searches for later retrieval. I am also aware that providers may also keep records of the webpages or IP addresses that a user clicks on or types directly into his web browser's address bar (as opposed to the provider's search bar), if the user is using the provider's web browser (e.g., Google Chrome) and has logged into the web browser with his email account's username and password.

112. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account.

Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

113. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

114. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email

providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

115. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling investigators to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the

geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

BACKGROUND CONCERNING SERVERS

116. Server providers like Digital Ocean maintain server computers connected to the Internet. Their customers use those computers for a wide range of different purposes, including operating websites and providing cloud-based data storage. In general, providers like Linode ask each of their customers to provide certain identifying information when registering for services, including name, contact information, email address and business information. Providers like Linode also may retain records of the length of service (including start date) and types of services utilized. In addition, for paying customers, such companies typically retain information about the customers' means and source of payment for services (including any credit card or bank account information).

117. Server providers' customers typically place files, software code, databases and other data on the servers. To do this, customers connect from their own computers to the server computers across the Internet. This connection can occur in several ways. In some situations, it is possible for a customer to upload files using a special web site interface offered by the server provider. It is frequently also possible for the customer to directly

access the server computer through the Secure Shell ("SSH") or Telnet protocols. These protocols allow remote users to type commands to the web server. The SSH protocol can also be used to copy files to the server. Customers can also upload files through a different protocol, known as File Transfer Protocol ("FTP"). Servers often maintain logs of SSH, Telnet and FTP connections, showing the dates and times of the connections, the method of connecting, and the IP addresses of the remote users' computers (IP addresses are used to identify computers connected to the Internet). Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports.

118. The servers use those files, software code, databases and other data to respond to requests from Internet users for pages or other resources from the website. Commonly used terms to describe types of files sent by a server include HyperText Markup Language ("HTML") (a markup language for web content), Cascading Style Sheets ("CSS") (a language for styling web content), JavaScript (a programming language for code run on the client's browser), and image files. Server providers frequently allow their customers to store collections of data in databases. Software running on the server maintains those databases; two common such programs are named MySQL and PostgreSQL, although those are not the only ones.

119. Server providers sometimes provide their customers with email accounts; contents of those accounts are also stored on the company's servers.

120. Web sites deliver their content to users through the Hypertext Transfer Protocol ("HTTP").6 Every request for a page, image file, or other resource is made through an HTTP request between the client and the server. The server sometimes keeps a log of all of these HTTP requests that shows the client's IP address, the file or resource requested, the date and time of the request, and other related information, such as the type of Web browser the client uses.

121. Websites are often known to the outside world by a domain name, such as www.uscourts.gov or www.amazon.com. Domain names must be registered to particular individuals or entities. Sometimes, server providers offer customers the separate service of registering domain names. When that occurs, server providers typically retain information related to the domain name, including the date on which the domain was registered, the domain name itself, contact and billing information for the person or entity who registered the domain, administrative and technical contacts for the domain, and the method of payment tendered to secure and register the domain name.

122. In some cases, a subscriber or user will communicate directly with a server provider about issues relating to a website or account, such as technical problems, billing inquiries or complaints from other users. Server providers typically retain records about such communications, including records of contacts between the user and the company's support services, as well as records of any actions taken by the company or user as a result of the communications.

---

[6] This includes secure forms of HTTP, such as HTTPS.

BACKGROUND CONCERNING DROPBOX

123. Dropbox is a service that allows its users to store files on Dropbox's servers. According to Dropbox's privacy policy, at https://www.dropbox.com/privacy, Dropbox collects and stores "the files you upload, download, or access with the Dropbox Service," and also collects logs: "When you use the Service, we automatically record information from your Device, its software, and your activity using the Services. This may include the Device's Internet Protocol ("IP") address, browser type, the web page visited before you came to our website, information you search for on our website, locale preferences, identification numbers associated with your Devices, your mobile carrier, date and time stamps associated with transactions, system configuration information, metadata concerning your Files, and other interactions with the Service. "Dropbox is a free service that lets you bring all your photos, docs, and videos anywhere. This means that any file you save to your Dropbox will automatically save to all your computers, phones and even the Dropbox website."

CONCLUSION

124. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require each of the Providers to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

125. Based on the forgoing, I request that the Court issue the proposed search warrants.

REQUEST FOR SEALING

126. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

127. Pursuant to 18 U.S.C. § 2705(b) and for the reasons stated above, it is further requested that the Court issue Orders commanding each of the Providers not to notify any person (including the subscribers and customers of the accounts listed in the warrant) of the existence of the warrant until further order of the Court.

Respectfully submitted,

EVELINA ASLANYAN
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on June 23, 2017

Honorable Lois Bloom
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following accounts that is stored at premises controlled by the respective Providers, each of which is a company that accepts service of legal process in the United States.

Account Identifier	Provider
a@mediamethane.com	Google
a@mediamethane.com	LinkedIn
"adw0rd"	Atlassian
alex@adzos.com	Google
alex@tipsters.com	Google
assembla@betaggregator.com	Google
Dropbox User ID 94568916	Dropbox
Google Analytics Account 12145724	Google
[redacted]	Google
ibetters2@gmail.com	Google
loscritino@gmail.com	Google
"mathete"	Atlassian
"nastra"	Atlassian
qoqenator@gmail.com	Google
sergey@adzos.com	Google
support@adzos.com	Google

tech@clickandia.com	Google
x11org@gmail.com	Google

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all messages, chats and/or emails associated with the account, including stored or preserved copies of messages sent to and from the account, draft messages, the source and destination addresses associated with each message, the date and time at which each message was sent, and the size and length of each message;

b. The text of all Internet search requests input by the subscriber; and all URLs or IP addresses typed into the browser address bar or URLs or IP addresses clicked on;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All accounts associated with the account (including all accounts accessed by the brower(s) and device(s) associated with the account), as determined by an analysis of cookies and/or machine cookies;

e. The types of service utilized;

f. Any unique identifiers that would assist in identifying device(s) associated with the account, including push notification tokens associated with the account (including Apple Push Notification (APN), Google Cloud Messaging (GCM), Microsoft Push Notification Service (MPNS), Windows Push Notification Service (WNS), Amazon Device Messaging (ADM), and Baidu Cloud Push);

g. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, files, and postings;

h. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

i. With respect to Google Analytics Account 12145724, all analytics and tracking data associated with this account and all of its associated Tracking IDs; and

j. With respect to Google Analytics Account 12145724, all of the information specified in items a. through h. with respect to each associated Tracking ID.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1030(a)-(b) (computer fraud and conspiracy and attempt to commit the same), 1343 and 1349 (wire fraud and wire fraud conspiracy), those violations involving the user(s) of the account(s) listed in Attachment A, his/her co-conspirators, associates and others with whom he/she has communicated, and occurring between July 1, 2014 and June 23, 2017, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Committing computer fraud, wire fraud, or conspiring or attempting to commit any of the foregoing, including the creation and operation of botnets, and the committing of click fraud, digital video advertising fraud, and other types of advertising fraud;

(b) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the account about matters relating to computer fraud, wire fraud, and conspiracy or attempt to commit any of the foregoing, including records that help reveal their whereabouts.